

NASA/TM—2001-210937



Using CORBA Sec to Secure Distributed Aerospace Propulsion Simulations

Tammy M. Blaser
Glenn Research Center, Cleveland, Ohio

May 2001

The NASA STI Program Office . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program Office plays a key part in helping NASA maintain this important role.

The NASA STI Program Office is operated by Langley Research Center, the Lead Center for NASA's scientific and technical information. The NASA STI Program Office provides access to the NASA STI Database, the largest collection of aeronautical and space science STI in the world. The Program Office is also NASA's institutional mechanism for disseminating the results of its research and development activities. These results are published by NASA in the NASA STI Report Series, which includes the following report types:

- **TECHNICAL PUBLICATION.** Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA's counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.
- **TECHNICAL MEMORANDUM.** Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.
- **CONTRACTOR REPORT.** Scientific and technical findings by NASA-sponsored contractors and grantees.

- **CONFERENCE PUBLICATION.** Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or cosponsored by NASA.
- **SPECIAL PUBLICATION.** Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.
- **TECHNICAL TRANSLATION.** English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services that complement the STI Program Office's diverse offerings include creating custom thesauri, building customized data bases, organizing and publishing research results . . . even providing videos.

For more information about the NASA STI Program Office, see the following:

- Access the NASA STI Program Home Page at <http://www.sti.nasa.gov>
- E-mail your question via the Internet to help@sti.nasa.gov
- Fax your question to the NASA Access Help Desk at 301-621-0134
- Telephone the NASA Access Help Desk at 301-621-0390
- Write to:
NASA Access Help Desk
NASA Center for Aerospace Information
7121 Standard Drive
Hanover, MD 21076

NASA/TM—2001-210937



Using CORBA Sec to Secure Distributed Aerospace Propulsion Simulations

Tammy M. Blaser
Glenn Research Center, Cleveland, Ohio

Prepared for the
Fifth Workshop on Distributed Objects and Components Security
sponsored by the Software Solutions Division of Hitachi Computer Products, Inc.
Annapolis, Maryland, March 26–29, 2001

National Aeronautics and
Space Administration

Glenn Research Center

May 2001

Trade names or manufacturers' names are used in this report for identification only. This usage does not constitute an official endorsement, either expressed or implied, by the National Aeronautics and Space Administration.

Available from

NASA Center for Aerospace Information
7121 Standard Drive
Hanover, MD 21076

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22100

Available electronically at <http://gltrs.grc.nasa.gov/GLTRS>

USING CORBASEC TO SECURE DISTRIBUTED AEROSPACE PROPULSION SIMULATIONS

Tammy M. Blaser
National Aeronautics and Space Administration
Glenn Research Center
Cleveland, Ohio 44135

NASA Glenn Research Center and its industry partners are developing a CORBASec test bed to secure their distributed aerospace propulsion simulations. NASA Glenn Research Center is an active domain member of the OMG and has been working with its aerospace propulsion industry partners to deploy the Numerical Propulsion System Simulation (NPSS) object based technology. When the NPSS is deployed, it will assemble a distributed aerospace propulsion simulation scenario from proprietary analytical CORBA servers and execute them with security afforded by the CORBASec implementation.

The NPSS CORBASec test bed will integrate the Hitachi TPBroker Security Service (SS) product, initially using the TPBroker Basic Object Adaptor (BOA) based ORB, with its NPSS software across different firewall products. The test bed will migrate to the Portable Object Adaptor (POA) architecture after Hitachi ports their SS to the VisiBroker 4.x ORB. NASA Glenn Research Center, General Electric Aircraft Engines and Pratt & Whitney Aircraft are the initial industry partner contributors to the NPSS CORBASec test bed.

The test bed is expected to demonstrate NPSS CORBASec specific policy functionality, confirm adequate performance and validate the required Internet configuration in a distributed collaborative aerospace propulsion environment.



Using CORBA^{Sec} to Secure Distributed Aerospace Propulsion Simulations

**NPSS CORBA^{Sec} Test Bed
DOCsec 2001**

March 28, 2001

NASA Glenn Research Center

Tammy M. Blaser

Tammy.M.Blaser@grc.nasa.gov

NPSS CORBASec Test Bed

Presentation Overview

- Motivation and Goal of the NPSS CORBASec Test Bed
- NPSS CORBASec Architecture *
- NPSS CORBA Wrapped Architecture *
- Schedule Phased Buildup
- Tools Current, Planned and for Future Study
- Preliminary Phase 1 of 4 Test Results and Environment
- Issues for OMG Attention
- Summary

* NPSS Dev Kit supports wrapping NPSS simulations with CORBA/CORBASec

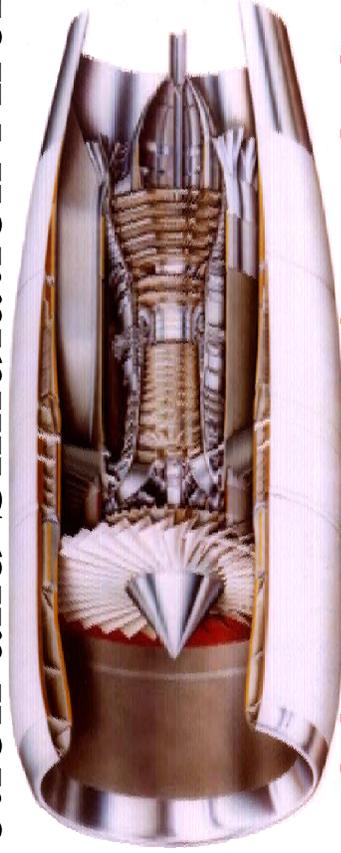
NPSS CORBASec Test Bed

Motivation and Goal of the NPSS CORBASec Test Bed

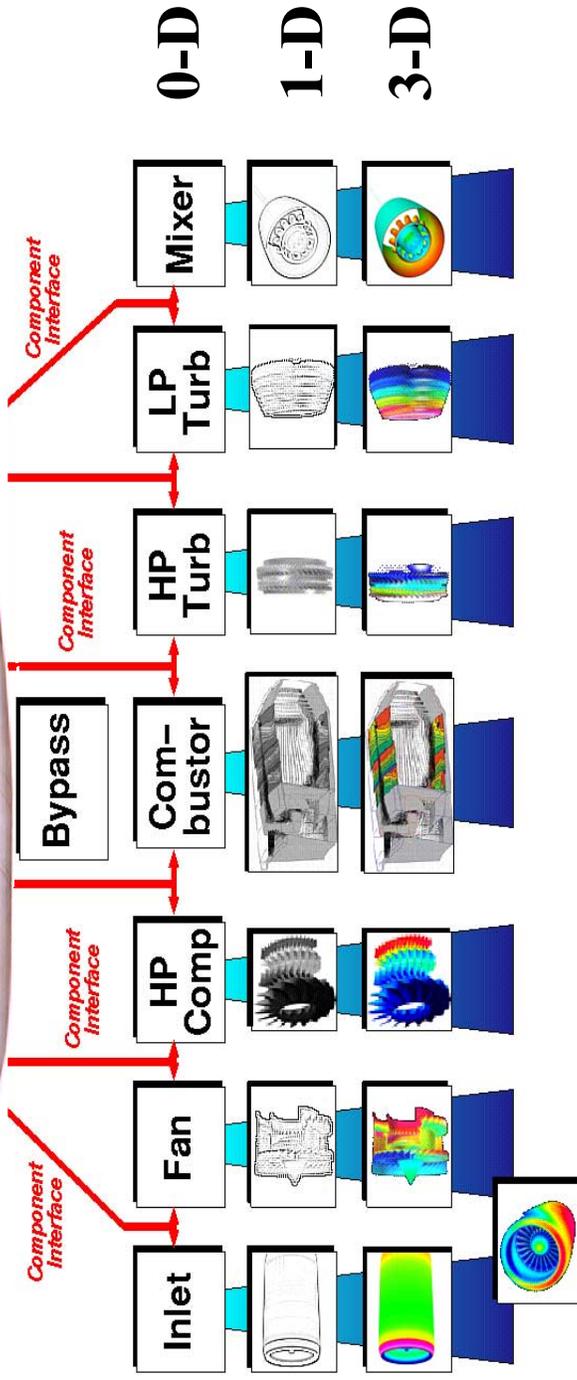
- Develop a test bed using CORBASec software and other security tools (firewalls, etc.) to secure NASA Glenn and cooperative industry partners distributed numerical propulsion simulations.
- Test bed results will drive the Numerical Propulsion System Simulation (NPSS) CORBASec production development and deployment
 - NPSS is part of the High-Performance Computing and Communications (HPCC) Program
- The NPSS allows various aerospace companies and NASA Glenn and NASA Ames to simulate a full-scale system engine at various levels of fidelity (0D, 1D, 3D and back)
 - NPSS is built following the Object Oriented Paradigm using C++ and CORBA
 - Java developments growing rapidly (EJB based Web Servers, GUIs for testing, ...)

NPSS CORBASec Test Bed

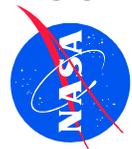
NPSS Production and Simulation Architecture



NPSS Production System Model



NPSS Dev. Kit supplies tools for integrating codes, accessing geometry, zooming, coupling, security.



Computing and Interdisciplinary Systems Office
Glenn Research Center

Collaborate on Multiple Component Architecture

- Collaborative/Multiple Domain First Phase Users:
 - NASA Glenn Research Center
 - Company 1
 - Company 2
- Multiple commercial ORBs, supporting CORBASec ORB Interoperability, will be implemented in the final phases (scheduling details in later slides)
- Exercising use of the SSL for on wire encryption (3DES) with CORBASec.
- Multiple Authentication techniques implemented and planned.
- NPSS Simulation developers use a CORBASec enhanced NPSS API Development Kit to enable and deploy CORBASec.
- Configured with multiple Firewalls.



Primarily CORBASec Security-Unaware Architecture

- Primarily uses CORBASec Security-Unaware (Enabled) *interceptor invoked* services
 - Simulation and Interpreter Interfaces with required privileges (rights) for public access
 - Security Policy Administered at Interface level with required rights for public access.
 - No methods configured for Security Policy Administration.
 - NPSS Access Control (AC) Administered based on the following combined attributes:
 - Aerospace Company or NASA Agency
 - Domain
 - Citizenship
 - Project
 - Role
 - General Users, Developers, and Restricted Users assigned privileges (rights):
 - » Private access limited to General Users and Developers (General Users have read-only private access)
 - » Public access granted to all User Roles (per Domain Access Policy)
 - » Restricted Users limited to Public access



Plus CORBASec Security-Aware

- 100% CORBASec Security-Unaware was our design goal, but ...
- NPSS AC proved runtime bound, therefore our design added a CORBASec Security-Aware *application invoked* “hook” and the Authorization (SecBuddy) Server was born.
- SecBuddy uses simple delegation and supports NPSS Client private access for dynamically invoked runtime bound operations.
 - via one hasPrivateAccess method call
 - Easy to update per application or security policy changes vs. changing multiple CORBASec Security-Unaware (Enabled) redundant methods
 - Old design had redundant methods get_public, get_private, set_public, set_private ...
 - Low coupling with CORBASec Administration
 - Supports growth and scalability



NPSS CORBASec Test Bed

Application Invoked AC

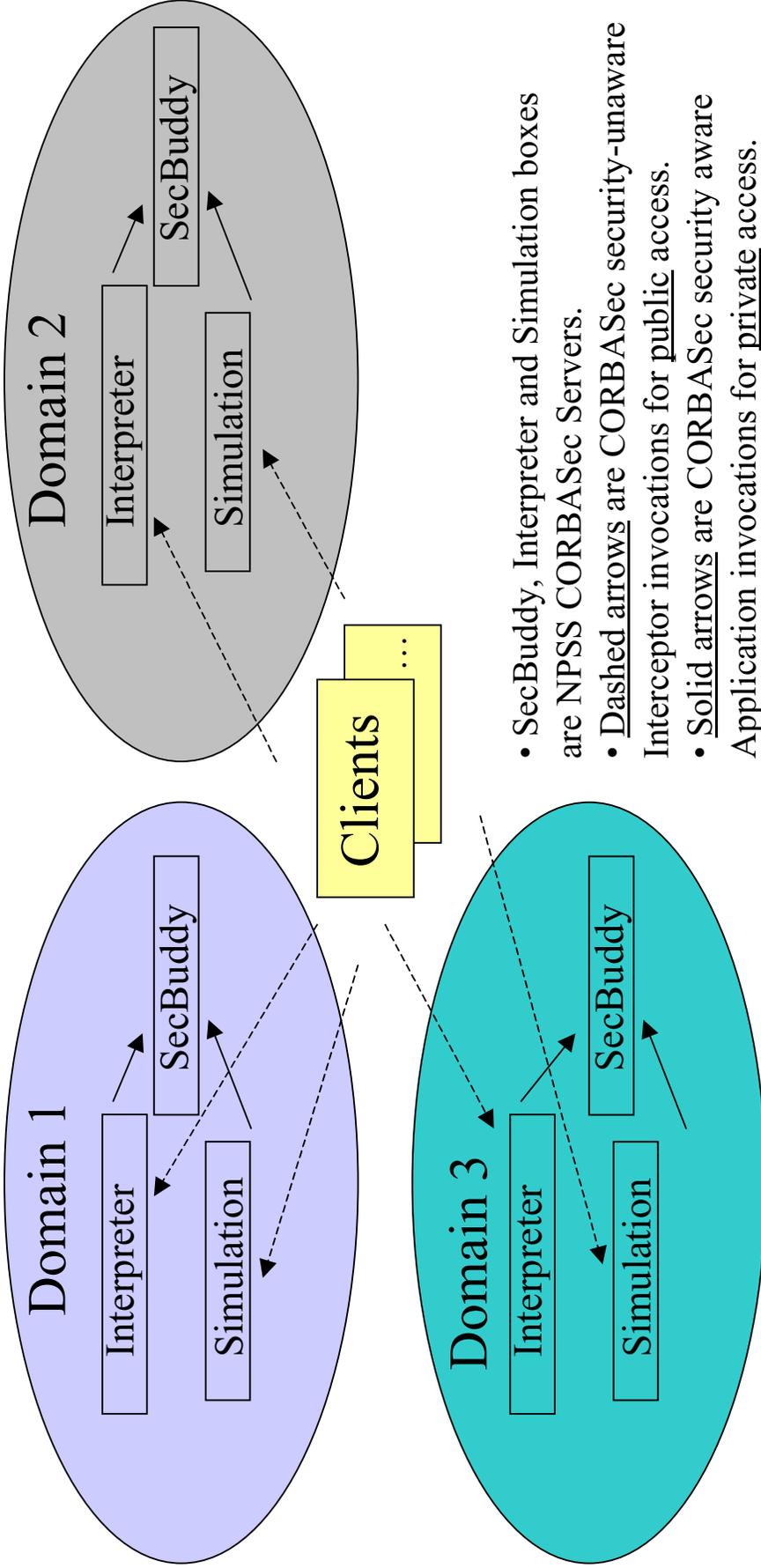
- Requires an Application System (NPSS Simulation, SecBuddy and Interpreter Servers) to be trusted (exercising formal application code inspections) to enforce NPSS AC decisions.
- SecBuddy Server, in a final configuration, will deploy a fault-tolerance design to make up for its dependence on Application invocation.



NPSS CORBASec Test Bed

NPSS Dynamic AC

Using CORBASec interceptor services and application invoked Architecture



NPSS CORBAsSec Test Bed

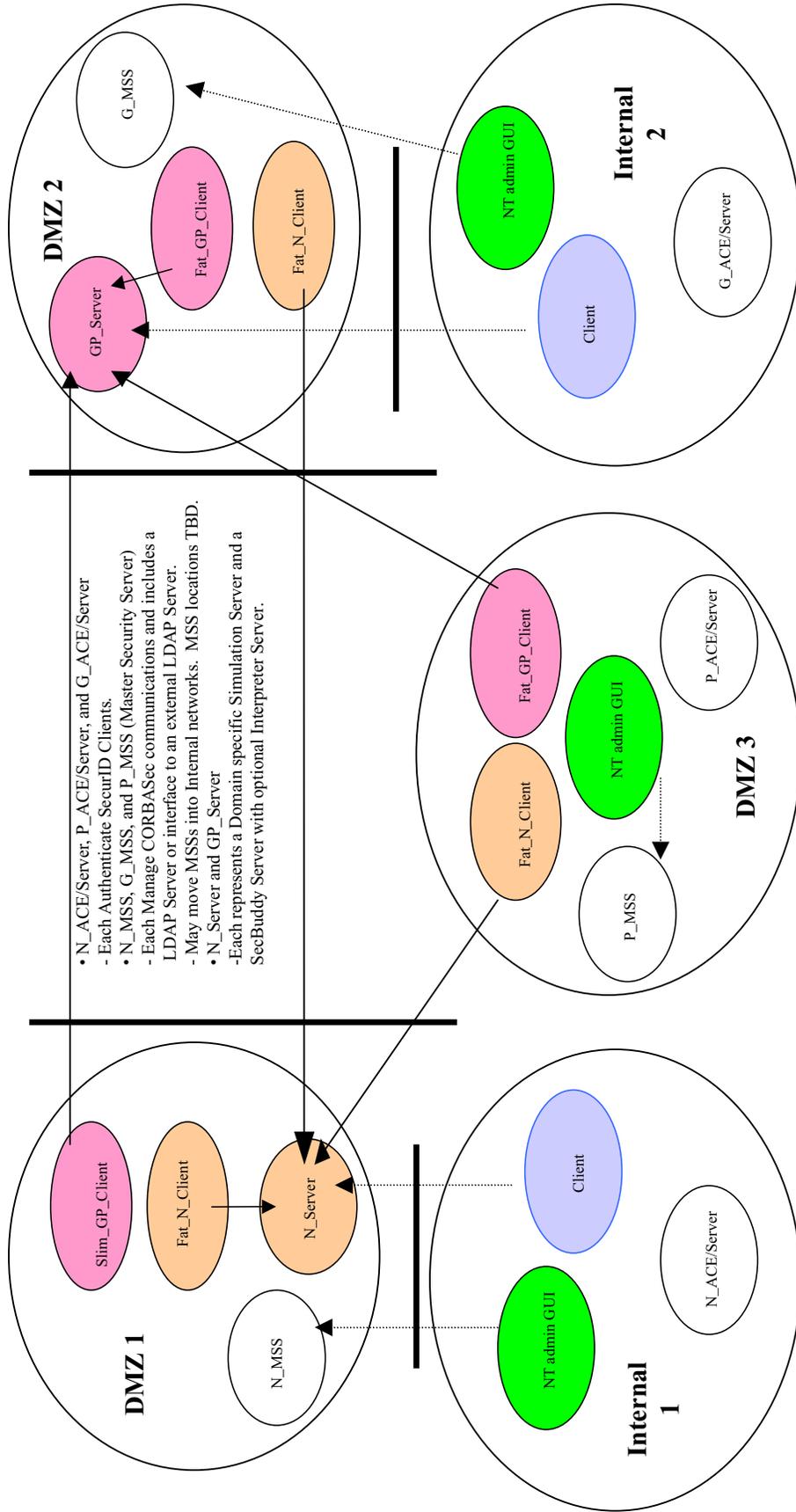
NPSS CORBAsSec Test Bed Example IDL

```
module npssCORBA {
  interface npssObject {
    // Every npss object can hold a table of protected variables. Security Policy is not directly Administered for Interface npssObject.
    string get(in string varName);
    boolean set(in string varName,
               in boolean isPrivate); // Many other npssObject methods exist in the production IDL
  };
  interface Interpreter: npssObject {
    // Security Policy Administered for the Interpreter Interface at the Interface level (not at parseString method) with required rights for public access.
    boolean parseString(in string cmdLine);
  };
  interface Simulation: npssObject {
    // Security Policy Administered for the Simulation Interface at the Interface level with required rights for public access.
    boolean runSim();
  };
  interface SecBuddy {
    // Security Policy Administered at Interface level with required rights. Includes one method hasPrivateAccess with required rights for private access.
    void hasPrivateAccess();
  };
};
```



NPSS CORBASec Test Bed

NPSS CORBASec Test Bed Phase 1 Firewall Architecture



- N_ACE/Server, P_ACE/Server, and G_ACE/Server
- Each Authenticate SecurID Clients.
- N_MSS, G_MSS, and P_MSS (Master Security Server)
- Each Manage CORBASec communications and includes a LDAP Server or interface to an external LDAP Server.
- May move MSSs into Internal networks. MSS locations TBD.
- N_Server and GP_Server
- Each represents a Domain specific Simulation Server and a SecBuddy Server with optional Interpreter Server.



Integrated SecurID NPSS Client Authentication

- SecurID is two-factor authentication that is based on something you know (a password or PIN), and something you have (an authenticator; we use key token fobs known for their light-weight and compact size). The SecurID token generates a new, unpredictable access code every 60 seconds.
- Currently testing a SecurID workaround prototype that uses the RSA ACE/Server authentication API to integrate SecurID-based authentication with Hitachi's TPBroker Security Service 3.4 Login API.
- The ACE/Server authentication API was provided as C libraries.
 - NASA has wrapped the SecurID authentication API methods for use with NPSS & CORBASec using C++.
- The code looks something similar to the following:

```
NPSS prototype client {  
    Do SecurID login           // Call ACE/Server authentication APIs  
    If failed, exit  
    Do Security Service login  // Call Security Service login API (necessary to create Credentials)  
    If failed, exit           // Processing can continue only if both authentications succeed  
    Continue with processing  
}
```

- After Hitachi Security Service 4.0 has implemented SecurID authentication

```
NPSS 4.0 client {  
    Do Security Service login  // Call Security Service login API now integrated with SecurID  
    If failed, exit  
    Continue with processing   // Processing can continue if authentication succeeds  
}
```



NPSS CORBA Wrapped Architecture

- NPSS is a component-based object oriented engine simulator.
- NPSS supports the use of external codes to extend a simulation to a higher fidelity and/or multidisciplinary analysis.
- Codes are CORBA wrapped to allow communication between NPSS and external codes.
- External codes use a direct CORBA wrapping scheme.
- Direct CORBA wrapping is accomplished via the easy to use NPSS Dev Kit (NPSS API for CORBA developers)
 - Transparent to the NPSS CORBA developer the API modifies the external code to become a CORBA Server conforming to the npssCORBA IDL
- The test bed results will provide the development roadmap required to add production grade CORBASec to the NPSS Dev Kit.



NPSS CORBASec Test Bed

Schedule Milestones Phased Buildup

- Developed in four phases.
- Preliminary results of the NPSS CORBASec Test Bed first phase effort, will be available in March 2001, at that time, the NPSS software team will finalize the NPSS Dev Kit detail design using the BOA based CORBASec and using the POA based CORBA Server.
- The second phase will be completed in June 2001 and will support the POA CORBASec architecture and NPSS training events; to include a Dry Run of NPSS Dev Kit Training.
- A release of CORBASec will be provided for the majority of the NPSS platforms with the November NPSS Release.
- The third phase will be completed in December 2001 and will support the POA CORBA architecture and NPSS Dev Kit Training.
- The NPSS Onsite is scheduled in December 2001.
- The fourth and final phase release will support all NPSS platforms and will be provided in the February 2002 NPSS Release.
 - Due to a recent project budget cut back the final NPSS CORBASec release is expected to slip 4-6 months.



Computing and Interdisciplinary Systems Office
Glenn Research Center

NPSS CORBASec Test Bed

Tools Current

- Solaris 2.6 (2.8 - later phases)
- Hitachi TPBroker Security Service (SS) for Java and C++ 3.4
- Hitachi TPBroker (VisiBroker repackaged/hardened (BOA) ORB) for Java and C++ 3.x
- LDAP iPlanet Directory Server 4.12
- Sun JDK 1.2 (1.3 – later phases)
- Sun Sparcworks 5.0 C++ compiler
- RSA ACE Server and Agent v.4.1 for Solaris
- NAI Gauntlet 5.5 Firewall (6.0 – later phase)
- Checkpoint 4.0 Firewall



NPSS CORBASec Test Bed

Tools Planned

- In June, Phase 2 we will
 - Upgrade to Forte 6.1 C++ compiler.
 - Upgrade to Solaris 2.8.
 - Upgrade CORBASec using Hitachi SS 4 to POA based on VisiBroker 4.x. ORB.
- Phase 3 we will add
 - POA based on Orbix 2000 ORB using Hitachi SS for Orbix 2000.
 - Ports to HP/UX 11, Linux RedHat 6.2 and (NT 4 and/or Windows 2000)
 - Additional C++ compilers (HP aC++, GCC, Microsoft, ...)
- Phase 4 we will add
 - Port to Irix using MICO 2.3.4 ORB
 - Irix C++ compiler
 - MICOsec for NPSS CORBASec Irix implementation
 - EJB/J2EE Web Security (BEA WebLogic)
- Need to add software tools to support:
 - Security Policy Generation
 - Develop detailed Security Policy Plans
 - If an intruder breaks in will our policy be?
 - Shutdown or Track the intruder?



NPSS CORBASec Test Bed

Tools Planned/Recommended

- Intrusion Detection
 - Choose a Intrusion Detection System based on detailed NPSS Security Policy Plans
 - Recommend Security Interfaces between CORBASec Non-Repudiation and Intrusion Detection Systems
- Certification
 - FIPS 140-1
 - FIPS 140-2 - when approved will replace FIPS 140-1
 - References Common Criteria
 - RSA BSAFE Crypto-C FIPS 140-1 (level 1) Certified (Integrated in VisiBroker SSL Pack)
 - Common Criteria
 - Solaris 2.8 (EAL 4) certified, but what about CORBASec?
 - CORBASec not ready, but to meet near term NPSS schedule ...
 - Recommend SSL to be Common Criteria Certified. Why?
 - » ANSI X.9F is in the process of embracing FIPS 140
 - » IV&V good engineering assessment
 - Pursue SSL Common Criteria (EAL 3) Certification for:
 - » RSA BSAFE SSL-C and SSL-J (Integrated in VisiBroker SSL Pack)
 - » Baltimore Technologies KeyTools SSL (Integrated in Orbix 2000; beta now)



Computing and Interdisciplinary Systems Office
Glenn Research Center

Tools for Future Study

- Need to study potential of using other Authentication Controls:
 - PKI Digital Certificates/Smart Cards
 - Methods for managing multiple CA endorsed digital certificates
- Biometrics
 - Fingerprint
 - Retinal Scan
 - Iris Scan
 - Voice Recognition
 - Face Recognition



NPSS CORBASec Test Bed

Preliminary Phase 1 of 4 Test Results

- Test Build Up Approach:
 - CORBA only Site Specific
 - CORBASec Site Specific
 - CORBASec Collaborate Network
- Completed IOP proxy (CORBA only/non-CORBASec) tests between Site 1 DMZ (Firewall) and Internal network:
 - Tests Used Hitachi TPBroker Security Service example Client/Server s/w.
 - And NAI Gauntlet 5.5 Firewall IOP Proxy
- Completed plug proxy CORBASec tests between Site 1 DMZ (Firewall) and Internal network:
 - Test Used SecurID and CORBASec Login workaround prototype.
 - Test Checked Out our NPSS CORBASec Prototype.
 - With SecBuddy, Interpreter and Simulation NPSS CORBASec Servers with various Clients.
 - Used NAI Gauntlet 5.5 Firewall Plug Proxy
 - SSL Proxy not used until enhancements made and Firewall Traversal Specification Baselined.



Preliminary Phase 1 of 4 Test Environment

- Test bed effort requires coordination with many groups (networking, developers, system administrators, various companies, etc.)
 - Network engineers
 - Are the “keeper of the keys”
 - Do not know CORBA/CORBASec (but Network engineers are gaining elevation)
 - Understand Firewalls and VPNs
- Hitachi has proved to be a very professional company and their company policy is to actively work with the NPSS CORBASec project.
- Currently we are moving forward with our first set of collaborative (between companies) CORBASec tests.



Issues for OMG Attention

- No Standard SSL API
 - SSL API required for multi ORB vendor CORBASec.
 - SSL Portability interfaces implemented by Hitachi Security Service as they port to both VisiBroker 4.x and Orbix 2000 ORBs.
 - SSL Interoperability required for end-to-end communication between NPSS partners.
- No Standard LDAP API
 - LDAP API will reduce risk of integrating multiple LDAP Servers (Site and CORBASec specific).
- Need Firewall Traversal Specification Baseline
 - Forward Identity (Delegation) of Client/Server Credentials may be required for the NPSS Collaborative Project in later phases.
 - Bi-Directional GIOP



NPSS CORBASec Test Bed

Summary

- We are integrating a production grade CORBASec capability with our component-based object oriented engine simulator (NPSS)
 - Porting to
 - Commercial ORBs (VisiBroker 4.x and Orbix 2000)
 - C++ and Java
 - Multiple operating systems (Solaris, HP/UX, NT, Windows 2000 and Linux)
 - With dedicated MICOSec development for SGI Irix platform
- Our test bed effort is key to the safe use and success of the NPSS project in its deployment phase.



REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY <i>(Leave blank)</i>	2. REPORT DATE May 2001	3. REPORT TYPE AND DATES COVERED Technical Memorandum	
4. TITLE AND SUBTITLE Using CORBASec to Secure Distributed Aerospace Propulsion Simulations		5. FUNDING NUMBERS WU-725-10-31-00	
6. AUTHOR(S) Tammy M. Blaser			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) National Aeronautics and Space Administration John H. Glenn Research Center at Lewis Field Cleveland, Ohio 44135-3191		8. PERFORMING ORGANIZATION REPORT NUMBER E-12790	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) National Aeronautics and Space Administration Washington, DC 20546-0001		10. SPONSORING/MONITORING AGENCY REPORT NUMBER NASA TM-2001-210937	
11. SUPPLEMENTARY NOTES Prepared for the Fifth Workshop on Distributed Objects and Components Security sponsored by the Software Solutions Division of Hitachi Computer Products, Inc., Annapolis, Maryland, March 26-29, 2001. Responsible person, Tammy M. Blaser, organization code 7750, 216-433-2699.			
12a. DISTRIBUTION/AVAILABILITY STATEMENT Unclassified - Unlimited Subject Category: 07 Available electronically at http://gltrs.grc.nasa.gov/GLTRS This publication is available from the NASA Center for AeroSpace Information, 301-621-0390.		12b. DISTRIBUTION CODE	
13. ABSTRACT <i>(Maximum 200 words)</i> NASA Glenn Research Center and its industry partners are developing a CORBASec test bed to secure their distributed aerospace propulsion simulations. NASA Glenn Research Center is an active domain member of the OMG and has been working with its aerospace propulsion industry partners to deploy the Numerical Propulsion System Simulation (NPSS) object based technology. When the NPSS is deployed, it will assemble a distributed aerospace propulsion simulation scenario from proprietary analytical CORBA servers and execute them with security afforded by the CORBASec implementation. The NPSS CORBASec test bed will integrate the Hitachi TPBroker Security Service (SS) product, initially using the TPBroker Basic Object Adaptor (BOA) based ORB, with its NPSS software across different firewall products. The test bed will migrate to the Portable Object Adaptor (POA) architecture after Hitachi ports their SS to the VisiBroker 4.x ORB. NASA Glenn Research Center, General Electric Aircraft Engines and Pratt & Whitney Aircraft are the initial industry partner contributors to the NPSS CORBASec test bed. The test bed is expected to demonstrate NPSS CORBASec specific policy functionality, confirm adequate performance and validate the required Internet configuration in a distributed collaborative aerospace propulsion environment.			
14. SUBJECT TERMS Aerospace; Propulsion; Computer simulation; Computer information security; Computer security; Java; Internets; C++; Distributed interactive simulation			15. NUMBER OF PAGES 29
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT